EXHIBIT B

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

FILED LODGED
RECEIVED
MAR 02 2018
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA
BY DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The subject premises of 100 174th Street S., Spanaway, WA 98387, and subject person Donnie Barnes

Case No. MJ18-5047

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The subject premises and subject person as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, USC § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, USC § 2252(a)(4)(B)	Possession of Child Pornography
Title 18, USC § 2251(a)	Production of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT REESE E. BERG, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: March 2, 2018

Judge's signature

City and state: TACOMA, WASHINGTON

THERESA L. FRICKE, U.S. MAGISTRATE JUDGE

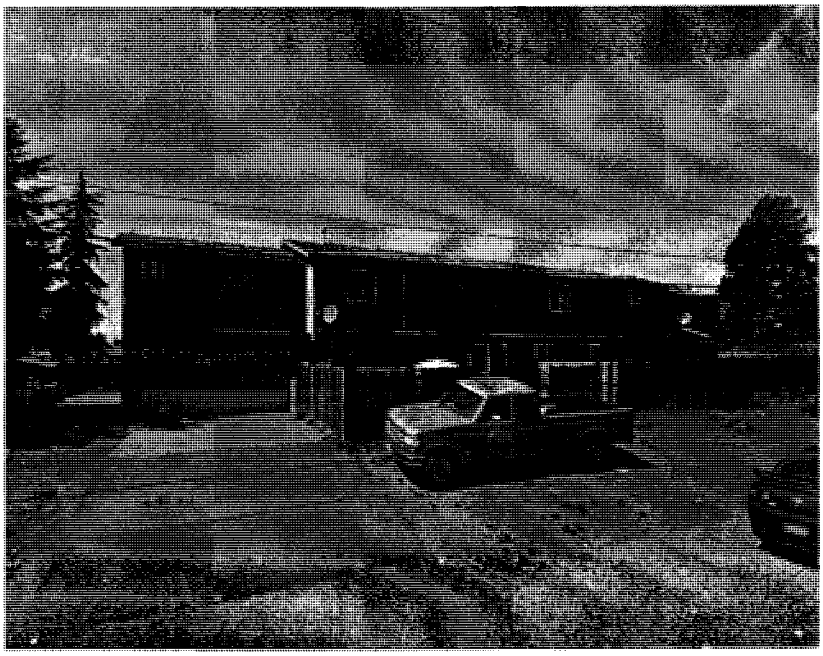
Printed name and title

2018R00227

ATTACHMENT A

Description of Property to be Searched

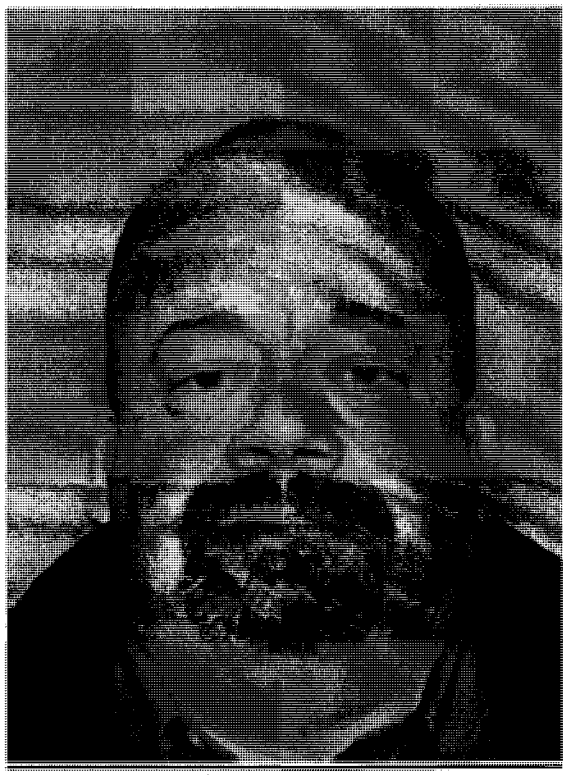
The SUBJECT PREMISES is the property located at 100 174th St. S., Spanaway, Washington 98387, and is more fully described as unit "100" of a blue in color two-story duplex with white trim that sits on the southwest corner of 174th St. S and A St. Unit 100 is on the south side of the duplex. The front door to the SUBJECT PREMISES is on the east side of the building and is white in color. The numbers "100" in a vertical fashion are posted directly below the exterior light fixture to the right of the garage door, and above the gate. The duplex is surrounded with a wood fence, with a gate leading to the front door. The garage for the SUBJECT PREMISES is on the southeast corner of the building and the door faces east.



The search is to include all rooms and persons within the SUBJECT PREMISES, vehicles located on the SUBJECT PREMISES, and all garage/parking spaces or storage units/outbuildings exclusively assigned to unit 100 and any digital device(s) found therein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The SUBJECT PERSON is Donnie Barnes Sr. (DOB: XX/XX/1967), pictured below:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP addresses 73.140.63.12 and 97.126.88.78 (the SUBJECT IP ADDRESSES) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Reese Berg, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7). I am currently employed as a Special Agent with Homeland Security Investigations (HSI). I have been a federal law enforcement officer for over 14 years. I have investigated and/or participated in investigations involving narcotics smuggling, human trafficking/smuggling, firearms trafficking, child pornography, child exploitation, marriage fraud and international criminal gangs. I have also held positions in law enforcement as a Military Police Officer and Military Police Investigator with the U. S. Army for over 20 years. I am a graduate of the 9-week Criminal Investigator Training Program as well as the Immigration and Customs Enforcement Special Agent Training program at the Federal Law Enforcement Training Center in Glynco, Georgia. I am currently assigned as a Special Agent with HSI Seattle, where my duties include child exploitation and child pornography investigations. I have participated in more than thirty child exploitation or child pornography investigations, and have worked extensively with other investigators involved in these types of investigations.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at 100 174th St. S., Spanaway, Washington (hereinafter the "SUBJECT PREMISES") more fully described in Attachment A, and the person of DONNIE BARNES, Sr. (the SUBJECT PERSON), for the things specified in Attachment B to this Affidavit, for the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

reasons set forth below. I also seek authority to examine digital devices or other electronic storage media. The property and person to be searched is as follows. The warrant would authorize a search of the SUBJECT PREMISES and persons within and the SUBJECT PERSON, as well as the seizure and forensic examination of digital devices found therein, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) will be found at the SUBJECT PREMISES, and on the SUBJECT PERSON.

5. Based on the discoveries I have made, as described below, I believe that an individual at the SUBJECT PREMISES has used a computer or other digital media device to connect to and access a foreign website that is well known to law enforcement and commonly used for child exploitation, via Internet Protocol (IP) addresses

73.140.63.12 and 97.126.88.78 and distributed at least one image depicting a minor engaged in sexually explicit conduct. I further believe that computers and other digital devices containing evidence of child pornography will be located at the SUBJECT PREMISES and/or on the SUBJECT PERSON.

II. STATEMENT OF PROBABLE CAUSE

A. Background of Investigation

6. In February 2018, HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) received a referral from the Queensland, Australia Police Service (QPS). On or about February 22, 2018, the lead was sent to the HSI Seattle office. The referral listed that the user of the account, TICK10TO12TOCK, had posted photos of a young female child to an album on a foreign public photo sharing website. The foreign public photo sharing website is known to me and other child exploitation investigators as a well-known online venue for pedophiles to communicate with each other and post/share albums of photos depicting children engaged in sexually explicit conduct. The profile indicated that TICK10TO12TOCK had been registered with the website since August 3, 2017.

7. On or about February 11, 2018, a QPS Officer working in an undercover (UC) capacity noticed a suspicious album on the foreign public photo sharing website, and posted a comment to a photo that TICK10TO12TOCK posted. The photo was in an album containing eleven other photos, all of which appeared to be of a young female. The QPS Officer commented, "oh wow, this is heaven! is this your own work?" User TICK10TO12TOCK replied less than two hours later "Yes it is." The photo in question, "IMG_1509.JPG", was posted by TICK10TO12TOCK along with two other photos, all of which appear to depict the same young girl.

8. I reviewed the file "IMG_1509.JPG" which is a close-up photo of the genital area of what appears to be a prepubescent female, hereinafter (female child victim) with olive skin tone. The female child victim is lying face down with a gray blanket partially between her legs and wearing blue panties. The panties appear to be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

manipulated as if they are being pulled to the right to expose the buttocks and genital area of the child. A portion of the genital area is visible, and I observed no pubic hair. This photo appears to be the second in a series of three photos posted by the user above. I also reviewed the other two photos described above, "IMG_1508.JPG" and "IMG_1510.JPG," each of which appear to depict the same child but from a slightly farther view, and the female child victim's underwear is in place. The female child victim appears to be wrapped in the same gray blanket as seen in "IMG_1509.JPG", with the portion of the blanket that would have been covering her buttocks area pulled upward. Copies of each of these images have been placed in an envelope, which will be Exhibit 1 to this Affidavit. Exhibit 1 will be made available to the reviewing magistrate judge but will not be filed with the Court and will instead be retained by HSI to be made available if relevant to a future legal proceeding.

9. On or about February 12, 2018, the QPS Officer received an email in reply to his comment on the photo. The email was from **dobsr@me.com,** and the name associated with the email was "Donnie Barnes". Below is the email exchange that transpired:

Donnie Barnes dobsr@me.com – *She's my sweet little toy.*

QPS Officer – *sorry mate, who are you on [foreign public photo sharing website]*

Donnie Barnes dobsr@me.com – *Tick10to12tock*

QPS Officer – *ah yes, ticktock!! what a great name to come up with. i love it. love your toy too! ile bet she tastes devine. please tell me more as I love to wank to stories*

i have a 11yo step dau myself but just startin off with her as i only met her mother online a month ago

just stealin some panties of hers to start off with & introducing her to french kissing

i don't do fantasys either so please be up front if she aint yours

thanks

alex

Donnie Barnes dobsr@me.com – *She is also my step daughter. She is 11 and very sexy. And very flirty. She is fun to play with. I can't tell stories right now but I will later on. Do you have a pic of your toy?*

QPS Officer – *ime at work now so cant send pics. i do have her panties though :) would love to go wank over her in the stall i my meal break. you ok with that? you got any pics to send?*

(NOTE - with this response, the QPS UC Officer attached three photos of soiled kid's panties)

Donnie Barnes dobsr@me.com – *Sounds fun to me.*

QPS Officer – *you got any more pics of her I can dribble some cum off? :) are you on any tor boards at all? ive been a member for a while now*

alex

With each email from Donnie Barnes dobsr@me.com, a footer to the email stating it was "Sent from my iPhone".

10. The QPS Officer obtained a list of IP logins for the account from the foreign public photo sharing website, which revealed that on numerous occasions between August 3, 2017, and February 20, 2018, the user TICK10TO12TOCK logged into the site. On October 3, 2017, at 11:00 (GMT), the user logged into the site utilizing the IP address 97.126.88.78 and again on February 20, 2018, at 13:45 (GMT) using IP address 73.140.63.12.

11. On February 21, 2018, HSI Intelligence Research Specialist (IRS) Lauren Morris issued a summons to CenturyLink requesting subscriber information for IP address 97.126.88.78 on October 3, 2017 at 11:00 (GMT).

12. On or about February 21, 2018, CenturyLink responded that IP address 97.126.88.78 was dynamically assigned, and on October 3, 2017, at 11:00 (GMT) was

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

assigned to J.B. at a residence in Tacoma, Washington. The account number was XXXXXXXXX1670, and the service was established on September 15, 2015.

13. On February 21, 2018, IRS Lauren Morris issued a summons to Comcast requesting subscriber information for IP address 73.140.63.12 on February 20, 2018, at 13:45 (GMT).

14. On or about February 21, 2018, Comcast responded that IP address 73.140.63.12 was dynamically assigned, and on February 20, 2018 at 13:45 (GMT) was assigned to K.T. at 100 174th St. S., Spanaway, Washington. The account number was XXXXXXXXXXXX3402, and the service was established on an unknown date. The email user id for the account was **dobsr@comcast.net**.

15. IRS Morris, through open source research, determined that the email address **dobsr@me.com** was linked to a Facebook profile, Donnie.Barnes.923.

16. IRS Morris reviewed the email metadata from the **dobsr@me.com** emails described above and determined the email user had used an iPhone to access the email account.

17. On February 22, 2018, I conducted open source and law enforcement record checks. I obtained Washington Department of Licensing (DOL) photos of both Donnie O. Barnes (XX/XX/1967) and K.T. (XX/XX/1982). I also obtained a list of vehicles associated with Donnie Barnes and K.T., one of which was a 2004 green Ford Expedition, Washington license BDF8424.

18. On February 27, 2018, I observed the green 2004 Ford Expedition, Washington license BDF8424, parked in the public parking lot of the Cintas facility at 631 Valley Ave. NW, Puyallup, Washington. Later, on the same date, I observed the same vehicle parked in the driveway of the SUBJECT PREMISES.

19. I reviewed the Facebook profile Donnie.Barnes.923, and the publically available profile picture shows the individuals whom I previously identified as Donnie Barnes (the SUBJECT PERSON) and K.T. through DOL photos. Donnie Barnes's profile page said he lives in Tacoma, Washington. In Donnie Barnes's friend list, I found

a link to K.T.'s Facebook profile. I looked at K.T.'s profile picture, and it also was a photo of Donnie Barnes and K.T.. The Facebook profiles for both indicate they work at Cintas Corporation.

20. In K.T.'s Facebook photos, I found a photo of two children: a young girl and boy.

21. I conducted a record check using law enforcement and publicly available databases for K.T.'s phone number listed on her Comcast account. That check showed this phone number was associated with the SUBJECT PREMISES.

22. In the early morning (6:30 a.m.) of February 28, 2018, I saw K.T. depart the SUBJECT PREMISES, along with two young children, a boy and a girl. The boy appeared to be 6-8 years old and girl appeared to be 9-12 years old. K.T. and the children were in a blue 2008 Honda SUV, Washington license 747YJK, which was registered to K.T. at 5210 N. 9th St., Tacoma, Washington. The green 2004 Ford Expedition, Washington license DF8424 that was parked at the SUBJECT PREMISES the previous evening had left prior to 5:30 a.m. when I arrived.

23. Later, on February 28, 2018, I went to the public parking lot of the Cintas facility listed above. In the parking lot, I observed Donnie Barnes and K.T. together in the smoking area talking with each other. I also saw in the parking lot the green 2004 Ford Expedition, Washington license BDF8424 and the blue 2008 Honda SUV, Washington license 747YJK.

24. On February 28, 2018, at 9:00 p.m., I observed both cars mentioned above parked in the driveway of the SUBJECT PREMISES.

25. On March 1, 2018, at 4:30 a.m., SA Ensley saw the green 2004 Ford Expedition, Washington license BDF8424 and the blue 2008 Honda SUV, Washington license 747YJK parked in the driveway of the SUBJECT PREMISES. Later that morning at 6:02 a.m., SA Ensley saw the SUBJECT PERSON get in the green 2004 Ford Expedition and leave the SUBJECT PREMISES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

26. As part of this application, I am seeking authority to execute this warrant before 6:00 a.m. Given the observations of the SUBJECT PERSON's morning routine described above, I believe they may depart for work prior to or near 6:00 a.m. I would prefer to execute this warrant while all occupants of the SUBJECT PREMISES are present. To maximize the chances of that being the case, I hope to execute this warrant between 4:00 and 6:00 a.m.

III. PRIOR EFFORTS TO OBTAIN EVIDENCE

27. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview with Donnie Barnes, or any other unknown resident(s) or occupant(s) of the SUBJECT PREMISES, they could rightfully refuse to give consent and the user who distributed child pornography files as outlined above could arrange for destruction of all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT PREMISES or the SUBJECT PERSON.

IV. TECHNICAL BACKGROUND

28. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet, the individual's IP address is visible to administrators of websites they visit. Further, the individual's IP address is broadcast during most Internet file and information exchanges that occur.

29. Based on my training and experience, I know that most ISPs provide only one IP address for each residential subscription. I also know that individuals often use multiple digital devices within their home to access the Internet, including desktop and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

laptop computers, tablets, and mobile phones. A device called a router is used to connect multiple digital devices to the Internet via the public IP address assigned (to the subscriber) by the ISP. A wireless router performs the functions of a router but also includes the functions of a wireless access point, allowing (wireless equipped) digital devices to connect to the Internet via radio waves, not cables. Based on my training and experience, today many residential Internet customers use a wireless router to create a computer network within their homes where users can simultaneously access the Internet (with the same public IP address) with multiple digital devices.

30. Based on my training and experience and information provided to me by computer forensic agents, I know that data can quickly and easily be transferred from one digital device to another digital device. Data can be transferred from computers or other digital devices to internal and/or external hard drives, tablets, mobile phones, and other mobile devices via a USB cable or other wired connection. Data can also be transferred between computers and digital devices by copying data to small, portable data storage devices including USB (often referred to as "thumb") drives, memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

31. As outlined above, residential Internet users can simultaneously access the Internet in their homes with multiple digital devices. Also explained above is how data can quickly and easily be transferred from one digital device to another through the use of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage devices (USB drives, memory cards, optical discs). Therefore, a user could access the Internet using their assigned public IP address, receive, transfer or download data, and then transfer that data to other digital devices, which may or may not have been connected to the Internet during the date and time of the specified transaction.

32. Based on my training and experience, I have learned that the computer's ability to store images and videos in digital form makes the computer itself an ideal repository for child pornography. The size of hard drives used in computers (and other digital devices) has grown tremendously within the last several years. Hard drives with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the capacity of four (4) terabytes (TB) are not uncommon. These drives can store thousands of images and videos at very high resolution.

33. Based on my training and experience, and information provided to me by other law enforcement officers, I know that people tend to use the same user names across multiple accounts and email services.

34. Based on my training and experience, collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by companies such as Google, Yahoo, Apple, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

35. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

36. Based on my training and experience, I have learned that producers of child pornography can produce image and video digital files from the average digital camera,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

mobile phone, or tablet. These files can then be easily transferred from the mobile device to a computer or other digital device, using the various methods described above. The digital files can then be stored, manipulated, transferred, or printed directly from a computer or other digital device. Digital files can also be edited in ways similar to those by which a photograph may be altered; they can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the child pornographer in that this method of production is a difficult trail for law enforcement to follow.

37. As part of my training and experience, I have become familiar with the structure of the Internet, and I know that connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

38. Based on my training and experience, I know that cellular mobile phones (often referred to as "smart phones") have the capability to access the Internet and store information, such as images and videos. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily connect the device to a computer or other digital device, via a USB or similar cable, and transfer data files from one digital device to another. Moreover, many media storage devices, including smartphones and thumb drives, can easily be concealed and carried on an individual's person and smartphones and/or mobile phones are also often carried on an individual's person.

39. As set forth herein and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

crimes that might be found at the SUBJECT PREMISES or on the SUBJECT PERSON, in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

40. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

41. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

42. Given the above-stated facts, and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the user who possessed and distributed child pornography file(s) to the foreign public photo sharing website and then discussed the circumstances of those images with undercover law enforcement in February 2018 likely has a sexualized interest in children and depictions of children and that evidence of child pornography is likely to be found on digital media devices, including mobile and/or portable digital devices that belong to this user or to which this user has access..

43. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may be stored on any digital device present at the SUBJECT PREMISES or on the SUBJECT PERSON.

44. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

45. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that if digital devices are found in the SUBJECT PREMISES or on the SUBJECT PERSON, there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

V. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

46. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

47. In this particular case, and in order to protect the third party privacy of innocent individuals residing in the residence, the following are search techniques that will be applied:

i. Device use and ownership will be determined through interviews, if possible, and through the identification of user account(s), associated account names, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

logons associated with the device. Determination of whether a password is used to lock a user's profile on the device(s) will assist in knowing who had access to the device or whether the password prevented access.

ii. Use of hash value library searches.

iii. Use of keyword searches, i.e., utilizing key words that are known to be associated with the sharing of child pornography.

iv. Identification of non-default programs that are commonly known to be used for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.

v. Looking for file names indicative of child pornography, such as, PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child pornography.

vi. Viewing of image files and video files.

vii. As indicated above, the search will be limited to evidence of child pornography and will not include looking for personal documents and files that are unrelated to the crime.

48. These search techniques may not all be required or used in a particular order for the identification of digital devices containing items set forth in Attachment B to this Affidavit. However, these search techniques will be used systematically in an effort to protect the privacy of third parties. Use of these tools will allow for the quick identification of items authorized to be seized pursuant to Attachment B to this Affidavit, and will also assist in the early exclusion of digital devices and/or files which do not fall within the scope of items authorized to be seized pursuant to Attachment B to this Affidavit.

49. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture.

50. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

VI. CONCLUSION

51. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography),

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located at the SUBJECT PREMISES or on the SUBJECT PERSON as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the location, vehicles, and person specified in Attachment A for the items more fully described in Attachment B.

Reese E. Berg, Affiant
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me this 2nd day of March, 2018. In addition to this affidavit, I have reviewed the images contained in Exhibit 1 to this affidavit. Upon reviewing the images, the envelope containing them was sealed, and I affixed my signature to a label placed across the seal.

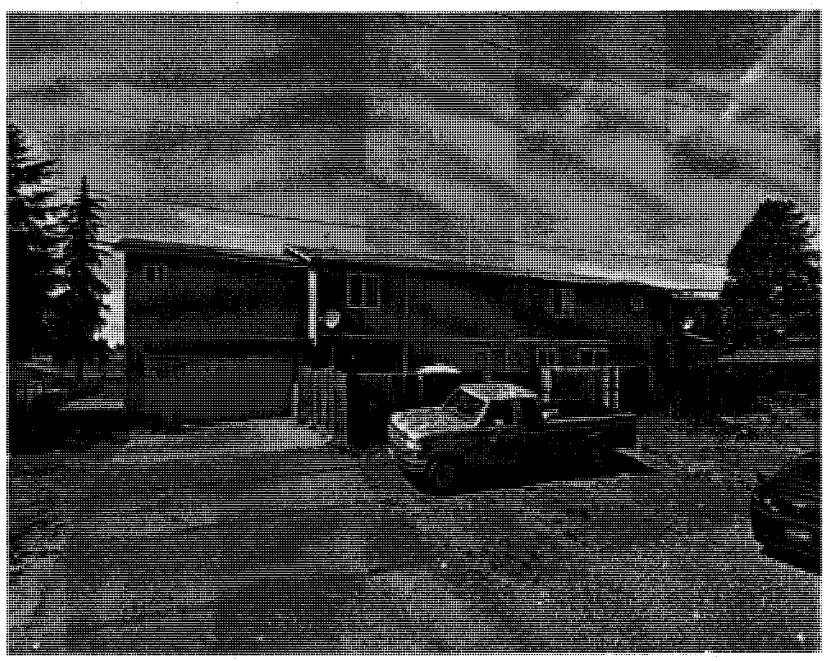
Theresa L. Fricke
THERESA L. FRICKE
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Description of Property to be Searched

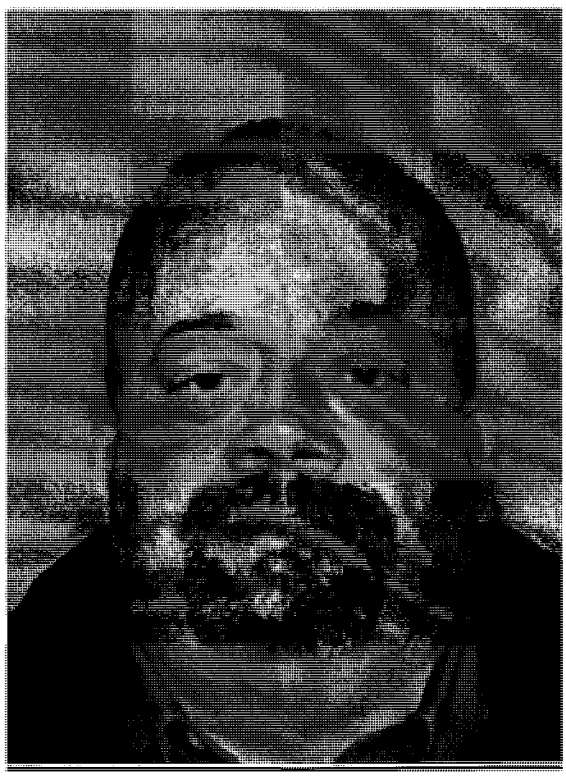
The SUBJECT PREMISES is the property located at 100 174th St. S., Spanaway, Washington 98387, and is more fully described as unit "100" of a blue in color two-story duplex with white trim that sits on the southwest corner of 174th St. S and A St. Unit 100 is on the south side of the duplex. The front door to the SUBJECT PREMISES is on the east side of the building and is white in color. The numbers "100" in a vertical fashion are posted directly below the exterior light fixture to the right of the garage door, and above the gate. The duplex is surrounded with a wood fence, with a gate leading to the front door. The garage for the SUBJECT PREMISES is on the southeast corner of the building and the door faces east.



The search is to include all rooms and persons within the SUBJECT PREMISES, vehicles located on the SUBJECT PREMISES, and all garage/parking spaces or storage units/outbuildings exclusively assigned to unit 100 and any digital device(s) found therein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The SUBJECT PERSON is Donnie Barnes Sr. (DOB: XX/XX/1967), pictured below:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP addresses 73.140.63.12 and 97.126.88.78 (the SUBJECT IP ADDRESSES) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970